REMARKS/ARGUMENT

Description of Amendments

Claims 1 and 12 are currently amended so as to include the features of claims 5 and 12, which are now canceled.

Claims 21 and 22 are new and serve to reinstate previously canceled claims 7 and 17.

Claims 1-4, 6, 8-15, 18, 19, 21 and 22 are pending after entry of this Amendment.

No new matter is introduced by this Amendment. Currently amended claims 1 and 12 are supported at least by the originally-filed specification corresponding to paragraph 42 of Pub. No. 2005/0209975 and original claims 5 and 12. New claims 21 and 22 are supported at least by original claims 7 and 17.

Reconsideration and removal of the rejections are respectfully requested.

Rejection under 35 U.S.C. §102

Claims 1, 3-6, 8-12, 14-16, and 18-20 were rejected under 35 U.S.C. §102(b) as being anticipated by U.S. Patent 6,105,008 ("*Davis*").

Independent claims 1 and 12 have been amended to include the elements of claims 5 and 12, respectively. Claims 5 and 12 are now canceled. *Davis* fails to teach the elements of claims 1 and 12 as amended. Accordingly, Applicant respectfully submits that claims 1 and 12 are patentably allowable over *Davis*.

Claim 1 as currently amended recites in relevant part: "a list containing information for authenticating the certificate of the second site is transmitted from the first site to the terminal via the network prior to receipt of the certificate by the terminal." Claim 12 as currently amended recites in relevant part: "wherein, prior to transmission of the certificate to the terminal, the site transmits to the terminal via the network a list containing information for authenticating the certificate." The Office contends that these elements of claims 1 and 12 are disclosed by *Davis*'s FIG. 11A. Applicant disagrees and respectfully submits that no portion of *Davis* discloses these elements of claims 1 and 12.

With regard to FIG. 11A, the Office explains: "reference number 606: allows client terminal to understand where to go for payment (part of the information sent is the IP address of the payment server), as well as the identities of the transaction and merchant using identifiers (allowing for further verification of the validity of the server)." *Id.* However, nothing in FIG. 11A nor in the associate written description in *Davis* teaches or suggests a list containing information that (1) is transmitted from the first site to the terminal via the network, and (2) is for authenticating the certificate of the second site.

The Office cites step 606 in FIG. 11A. In step 606, a merchant server builds an HTML page that includes various parameters mentioned by the Office above. *Davis* col. 12, lines 1-15. The HTML page is sent to a client terminal operated by a user. *Id.* col. 12, lines 15-18. Thus, the Office deems the claimed "first site" equivalent to *Davis*'s merchant sever (208), the claimed "terminal" equivalent to *Davis*'s client terminal (204), and the HTML page equivalent to the claimed "list of information." As explained below, however, the HTML page is not for authenticating a certificate of a second site, contrary to claim 1.

According to the Office, the claimed "second site" is met or disclosed by reference numbers 512 and 518 in *Davis*'s FIG. 10. Numbers 512 and 518 correspond to functions of a payment server. Thus, as best understood, the Office equates the claimed "second site" with *Davis*'s payment server (206). The relationships between *Davis*'s client terminal (204), payment server (206), and merchant server (208) are illustrated in *Davis*'s FIG. 5 (below).

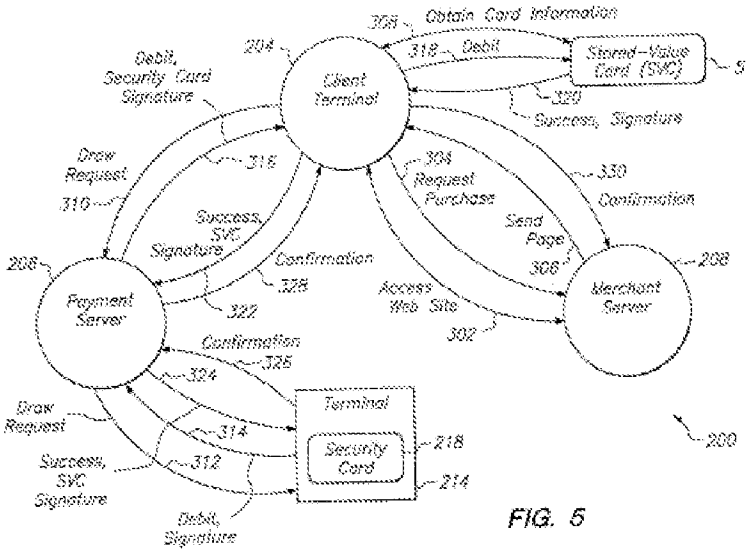

FIG. 5

First, the payment server (206) does not provide a certificate to the client terminal (204), contrary to claim 1. As can be seen in FIG. 5 above, the payment server transmits a communication to the client terminal at steps 316 and 328 involving a security card signature from the security card (218) and a confirmation -- none of these are a certificate. *Davis* col. 13, lines 26-29 and 41-43.

Second, even if the Office maintains that the payment server (206) sends a certificate to the client terminal (204), the HTML page sent by the merchant server to the client terminal is not for authenticating the alleged certificate. In FIG. 5 above, the step of sending the HTML page by the merchant server to the client terminal is shown as arrow 306. None of the subsequent steps, namely 308 and onward in FIG. 5, teach or suggest that the HTML page is used for authenticating a certificate of the payment server.

The Office states that the HTML page includes the IP address of the payment server. The IP address, however, is merely for allowing the client terminal to access the payment server and to send a draw request to the payment server (step 310 in FIG. 5). *Davis* col. 13, lines 15-18. The IP address is not for authenticating a certificate of the payment server. In fact, none of the other parameters or information in the HTML page mentioned in *Davis* col. 12, lines 2-15 is for authenticating a certificate of the payment server. Validation of the payment server side of the architecture of FIG. 5 is performed by means of a security card (218) and not by means of the HTML page sent by the merchant server. *Davis* col. 13, lines 30-34.

* * *

The Office requested that the Applicant to "fully consider the items of evidence in their entirety" since, according to the Office, the specific citations in the Final Action "are merely representative of the teaching of the prior art" and "other passages and figures may apply [to the claims] as well." *Final Action* pp. 6 & 7. Here, the only item of evidence presented is *Davis*. Applicant has fully considered *Davis* and has found no teaching or suggestion of the above quoted elements of claims 1 and 12 associated with authenticating a certificate from a second site. *Davis* discloses alternative embodiments of an internet payment architecture in FIGS. 6-9 and associated text. The alternative embodiments also use a security card (218) for validation purposes and do not use the HTML page or a list of information provided by the merchant server. Although the security card (218) is not shown

in FIG. 9, *Davis* col. 20, lines 42 and 58 indicate that the embodiment of FIG. 9 uses a security card for validation purposes and not a list of information provided by the payment server.

* * *

Davis also fails to teach other elements of claims 1 and 12.

With regard to the claimed elements associated with encrypting and decrypting, the Office states that "it is inherent in Internet transactions to encrypt and decrypt data, because security is an objective over a network such as the Internet." Under this reasoning, the Office contends that a feature that is desirable in a system is inherent in the system. The Office has applied the wrong standard. To establish inherency, "the examiner must provide a basis in fact and/or technical reasoning to reasonably support the determination that the allegedly inherent characteristic **necessarily** flows from the teachings of the applied prior art." MPEP 2112, quoting *Ex parte Levy*, 17 USPQ2d 1461, 1464 (Bd. Pat. App. & Inter. 1990) (emphasis in original). Not all communications over the Internet are encrypted. Therefore, encryption is not an inherent characteristic of communications over the Internet.

To anticipate a claim, "[t]he identical invention must be shown in as **complete detail** as is contained in the ... claim." MPEP 2131, quoting *Richardson v. Suzuki Motor*, 868 F.2d 1226, 1236, 9 USPQ2d 1913, 1920 (Fed. Cir. 1989) (Applicant's emphasis). The Office cites *Davis* col. 19, lines 33-47 and col. 21, lines 6-8. These and other passages in *Davis* describe a DES key shared by the payment and merchant servers, keys derived from the DES key, and a transaction session key created by the merchant server. Still, *Davis* fails to disclose the elements of claims 1 and 12 in complete detail.

With regard to claim 1, *Davis* fails to disclose: (1) a terminal having logic for decrypting the encrypted personal data using the **first key**, where the first key is provided by the secure device; and (2) the terminal having logic for re-encrypting the decrypted personal data with a **second key**. In *Davis*, the client terminal uses a single transaction session key received from the merchant server to decrypt and re-encrypt a debit command and does not use two separate keys for decrypting and encrypting. *Davis* col. 20, lines 46-53. The client terminal does not have access to another key. In particular, the client terminal does not have access to the DES key and derived keys. *Davis* col. 21, lines 3-8. For the same reasons,

Davis fails to disclose in complete detail a method in which personal data is decrypted and encrypted by a terminal by use of respective first and second keys as described in claim 12.

* * *

For the reasons given above, Applicant submits that independent claims 1 and 12 are patentably allowable over *Davis*.

Claims 3, 4, 6, 8-11, 14-16, and 18-20 depend from base claim 1 or 12 and thereby include all the elements of their respective base claim as well as additional elements. Accordingly, Applicant submits that claims 3, 4, 6, 8-11, 14-16, and 18-20 are patentably allowable over *Davis* for at least the same reasons given for claims 1 and 12.

Claims 5 and 12 are canceled, rendering their rejections moot.

Rejection under 35 U.S.C. §103

Claims 2 and 13 were rejected under 35 U.S.C. §103(a) as being unpatentable over *Davis* in view of Official Notice. Applicant traverses.

When Official Notice is taken, "[t]he examiner must provide specific factual findings predicated on sound technical and scientific reasoning to support his or her conclusion of common knowledge." MPEP 2144.03, B. The Office asserts that deactivating circuitry was old and well-known in the art "because it allows for a way to keep private information secure to even the most determined attackers." *Final Action* of April 28, 2008 pp. 5 & 6. The Office also asserts that "This solution provides a more secure system where data will not fall into an attacker's hands." *Id.* These and other statements in the *Final Action* surrounding the Official Notice are nothing more than asserted advantages and hypothetical motivations for arriving at the claimed invention and are not factual findings nor a technical line of reasoning. Accordingly, Applicant respectfully submits that the rejections of claims 2 and 13 are improper.

With regard to the substance of the Office's "factual findings," Applicant notes that a desire to make a device more secure does not necessarily lead to the features of claim 2 and 13. For instance, a device can be made more secure by encrypting a key contained in the device, by causing only the key contained in the device to be unreadable while allowing other

portions of the device to remain operable, or by making the device more robust against attack.

Conclusion

In light of the foregoing remarks, this application is considered to be in condition for allowance, and early passage of this case to issue is respectfully requested. If necessary to effect a timely response, this paper should be considered as a petition for an Extension of Time sufficient to effect a timely response, and please charge any deficiency in fees or credit any overpayments to Deposit Account No. 07-1850.

Respectfully submitted,

Date: July 25, 2008

/Norman Morales/

Norman Morales
Attorney for Applicant
Reg. No. 55,463

Squire, Sanders & Dempsey L.L.P.
One Maritime Plaza
Suite 300
San Francisco, CA 94111
Facsimile (415) 393-9887
Telephone (415) 393-09857
nmorales@ssd.com